

International Journal of Law, Human Rights and Social Sciences Research

Volume 2 | Issue 3, July-September 2026, pp. 28-33

ISSN (Online): 3139-406X

Homepage: <https://ijlhssr.com>



Title: From Protection to Participation: Reimagining Children's Rights in the Age of AI, Data Exploitation, and Transnational Cybercrime

Author(s): Dr. Mandeep Singh

Affiliation(s): Associate Professor, Rampur College of Law, Milak, Rampur (UP) India

DOI: <https://doi.org/10.65919/ijlhssr.2026.v2i3002>

History: Received: 21 May 2026, Accepted: 30 June 2026, Published: 10 August 2026

Citation: Singh, D. M. (2026). From Protection to Participation: Reimagining Children's Rights in the Age of AI, Data Exploitation, and Transnational Cybercrime. *International Journal of Law, Human Rights and Social Sciences Research*, 2(3). 28-33, <https://doi.org/10.65919/ijlhssr.2026.v2i3002>

Copyright: © 2026 The Author(s)

Licensing:  [Open access under CC BY-NC 4.0](https://creativecommons.org/licenses/by-nc/4.0/)

Conflict of Interest: The author(s) declare no conflict of interest.

Funding: This research received no specific grant from any funding agency in the public, commercial, or not-for-profit sectors.

Corresponding Author: Dr. Mandeep Singh 

Published By: [UnivColl Publications](https://univcollpublications.com)

From Protection to Participation: Reimagining Children's Rights in the Age of AI, Data Exploitation, and Transnational Cybercrime

Dr. Mandeep Singh

Associate Professor, Rampur College of Law, Milak, Rampur, UP

Abstract

The digital transformation of childhood has created a fundamental paradox: while online platforms offer unprecedented access to education, creativity, and global connectivity, they simultaneously expose children to systemic risks of exploitation, privacy violations, and algorithmic manipulation. This paper critically examines this "digital childhood dilemma" by analysing the adequacy of existing legal frameworks—from the United Nations Convention on the Rights of the Child (UNCRC) to India's Protection of Children from Sexual Offences (POCSO) Act, the Information Technology Act, 2000, the Digital Personal Data Protection Act (DPDP), 2023, and the European Union's General Data Protection Regulation (GDPR)—in addressing emerging threats such as AI-generated deep fakes, predatory data mining, dark web trafficking, and cross-border cybercrime. Using a doctrinal and comparative legal methodology, the study evaluates the gap between policy rhetoric and enforcement reality, particularly in developing nations like India, where rapid digital penetration outpaces institutional capacity. The findings reveal that current laws are predominantly reactive and punitive, failing to proactively safeguard children's participatory rights or hold technology corporations accountable for design-based harms, such as addictive interfaces, behavioural profiling, and inadequate age-verification systems. The paper proposes a holistic, child-centric framework that integrates legal reform, technological accountability, digital literacy, and international cooperation. It argues that effective protection cannot be achieved through surveillance and restriction alone; rather, it requires empowering children as digital citizens while imposing binding obligations on states and corporations to ensure safety-by-design, algorithmic transparency, and meaningful parental consent. The study concludes by advocating for a balanced regulatory approach that reconciles children's rights to protection, privacy, and

participation in an increasingly AI-driven and commercially exploitative digital ecosystem, drawing on best practices from the UK's Age Appropriate Design Code, the EU's GDPR, and emerging jurisprudence in Indian courts.

Keywords: Children's Rights, Artificial Intelligence (AI), Digital Childhood, Data Exploitation, Online Child Safety, Transnational Cybercrime, Data Privacy, Algorithmic Manipulation, Corporate Accountability, Digital Citizenship.

Introduction

1. The Digital Paradox: Opportunity Meets Vulnerability

The twenty-first century has birthed a generation for whom the digital and the physical are inseparable. From smart toys that learn a child's preferences to AI-tutoring systems that adapt to their learning pace, technology is no longer an external tool but an intrinsic part of childhood development. This digital immersion offers transformative potential: a child in a rural Indian village can access global knowledge repositories through platforms like DIKSHA or Khan Academy; young activists can mobilise for climate justice across continents using social media; and neurodivergent children can find affirming communities on specialised forums. The internet, in its ideal form, is a great equaliser—a democratic space where age, geography, and socio-economic status need not determine one's access to information or opportunity ^[1, 2].

However, this utopian vision is shadowed by a profound and escalating crisis. The same algorithms that recommend educational content also push addictive, harmful, or extremist material to impressionable minds. The same social platforms that enable self-expression also serve as hunting grounds for predators using AI to generate realistic grooming narratives ^[3]. The same data that personalises a child's experience is harvested, commodified, and weaponised by corporations and cybercriminals alike ^[4]. This is the digital childhood dilemma: the very architecture of the online world simultaneously enables empowerment and facilitates exploitation, often with the child caught in the crossfire of corporate profit motives and state surveillance. As the UN Committee on the Rights of the Child noted in General Comment No. 25, states must recognise that digital technologies are not neutral; they are designed environments that can either advance or undermine children's rights ^[5].

2. The Inadequacy of "Old" Laws in a "New" World

The legal response to this dilemma has been woefully inadequate. The United Nations Convention on the Rights of the Child (UNCRC), ratified in 1989, remains the gold standard for children's rights. Yet, its provisions—particularly Articles 16 (privacy), 17 (access to information), 19 (protection from violence), and 34 (protection from sexual exploitation)—were drafted in a pre-internet era. While General Comment No. 25 (2021) attempts to bridge this gap by explicitly addressing digital environments, its principles are non-binding and inconsistently applied across jurisdictions ^[6].

At the national level, laws such as India's POCSO Act (2012) and the IT Act (2000), the U.S. Children's Online Privacy Protection Act (COPPA, 1998), and even the EU's GDPR (2016)—while commendable in parts—are fundamentally reactive. They criminalise specific acts (e.g., sharing child pornography, unauthorised data collection) but fail to address the systemic vulnerabilities embedded in platform design: the attention economy that exploits children's dopamine responses, the algorithmic nudging that shapes their worldview, and the data brokerage industry that trades their digital identities without meaningful consent ^[7, 8].

Moreover, the transnational nature of digital threats renders domestic laws almost useless. A predator in one jurisdiction can target a child in another, using encrypted networks and AI-generated content that leaves no

forensic footprint. The dark web, decentralised finance, and the rise of the metaverse have created unregulated spaces where traditional law enforcement cannot reach^[9]. The result is a global protection deficit, where children's rights are routinely violated with impunity. As the Internet Watch Foundation reports, the volume of self-generated child sexual abuse material has skyrocketed, often facilitated by AI tools that can anonymise perpetrators and generate synthetic abuse imagery^[10].

3. The Corporate Accountability Gap

Perhaps the most glaring lacuna in the current discourse is the near-total absence of corporate accountability. Technology companies are not neutral conduits; they are active architects of children's digital environments. Their business models depend on maximising user engagement, which often translates to keeping children online for longer periods, exposing them to more ads, and collecting more data^[11]. Despite self-regulatory pledges and "safety" features, platforms consistently prioritise growth over protection. Age-verification systems are easily bypassed; content moderation is underfunded and biased; and "privacy-by-design" is often an afterthought rather than a foundational principle.

For instance, a study by the 5Rights Foundation found that major social media platforms failed to meet even basic child-safety benchmarks, including transparent reporting mechanisms and meaningful age checks^[12]. This paper argues that any effective solution must shift the burden of safety from parents and children to the corporations that design, deploy, and profit from these digital ecosystems. As the UN Committee on the Rights of the Child emphasised in General Comment No. 16, states have an obligation to regulate the business sector to prevent violations of children's rights, including in digital spaces^[13].

4. The Indian Context: A Microcosm of Global Challenges

India serves as a critical case study for this dilemma. With over 900 million internet users and one of the world's youngest populations—over 40% of its 1.4 billion people are under 18—India is both a vast market for digital services and a high-risk zone for online child exploitation^[14]. The government's push for "Digital India" has accelerated connectivity, but has not been matched by corresponding investments in digital literacy, cyber-policing, or child-sensitive legal infrastructure.

The newly enacted Digital Personal Data Protection Act (DPDP), 2023, introduces important provisions for children's data, including prohibitions on tracking, behavioural monitoring, and targeted advertising directed at minors, and requiring verifiable parental consent. However, its enforcement mechanisms are opaque, the definition of "parental consent" remains ambiguous, and its scope does not cover the full spectrum of cyber vulnerabilities—including AI-generated abuse, algorithmic discrimination, or cross-border content flows^[15]. Moreover, India has not ratified the Budapest Convention on Cybercrime, which limits its capacity for international cooperation in investigating and prosecuting transnational digital crimes^[16].

This paper examines the Indian legal landscape not in isolation but as a lens through which to understand the broader global struggle: how can developing nations balance the imperative of digital inclusion with the equally pressing need for robust child protection? As noted by Gasser, Maclay, and Palfrey, digital safety frameworks must be contextualised within local socio-cultural realities, infrastructural constraints, and legal traditions^[17].

5. Research Problem and Contribution

The central research problem addressed by this study is: How can children's rights be meaningfully reconciled with online safety in an era defined by AI-driven exploitation, commercial data extraction, and transnational

cybercrime? This question demands a multi-layered inquiry into legal adequacy, technological efficacy, and stakeholder responsibility.

The existing literature tends to treat these issues in silos—focusing on either cybercrime law, data privacy, or digital citizenship. For example, studies on child pornography often ignore data protection; studies on data privacy rarely address algorithmic harm; and studies on digital citizenship seldom engage with criminal law enforcement. This paper contributes a holistic, interdisciplinary synthesis that bridges these domains. It moves beyond a narrow focus on "abuse" to address the broader structural harms of the digital economy, including data exploitation, algorithmic manipulation, and the erosion of children's autonomy. It also foregrounds the role of AI as both a tool for protection (e.g., content moderation) and a vector of harm (e.g., deepfakes, generative CSAM), arguing that legal frameworks must be technologically adaptive rather than static ^[18].

6. Scope and Structure

The paper is organised into six substantive sections. Following this introduction:

- Section 2 explores the transformation of childhood in the digital age, mapping both the opportunities and the specific vulnerabilities created by AI, social media, and immersive technologies. It draws on sociological and psychological research to explain why children are uniquely susceptible to digital harms ^[19].
- Section 3 provides a critical analysis of international and national legal frameworks, including the UNCRC, GDPR, COPPA, India's POCSO Act, IT Act, and DPDP Act, identifying gaps, contradictions, and enforcement failures. A comparative table highlights jurisdictional differences ^[20].
- Section 4 examines the roles of key stakeholders—governments, tech companies, parents, educators, and civil society—highlighting failures and potential leverage points. It argues for a "multi-stakeholder accountability model" ^[21].
- Section 5 proposes a comprehensive framework for reform, centred on four pillars: (a) legal harmonisation and extraterritorial application, (b) corporate accountability and binding safety standards, (c) digital empowerment and critical literacy curricula, and (d) international cooperation through treaties and intelligence-sharing ^[22].
- Section 6 concludes by reflecting on the philosophical and ethical dimensions of protecting children in a world where their digital footprints are permanent, their data is currency, and their future is shaped by algorithms they cannot see or challenge. It calls for a paradigm shift from "protection from" to "protection for"—i.e., protecting children's rights to participate, create, and thrive online, not merely shielding them from harm ^[23, 24].

Author's Declaration & Publication Consent

The author(s) declare that the manuscript is original, accurate to the best of their knowledge, and does not knowingly infringe any copyright, privacy, or other third-party rights. All necessary permissions, ethical approvals, disclosures, and consents, where applicable, have been obtained. The author(s) accept responsibility for the content, data, interpretations, conclusions, authorship, and compliance with applicable research and publication ethics. Any conflicts of interest and funding sources have been appropriately disclosed. The author(s) authorize the Journal and Publisher to publish and disseminate the article under the Creative Commons Attribution-Noncommercial 4.0 International License (CC BY-NC 4.0).

Reference List

1. Livingstone, S., & Byrne, J. (2018). Parenting in the digital age: The challenges of digital parenting. UNICEF Office of Research.

2. UNICEF. (2017). The state of the world's children 2017: Children in a digital world. UNICEF.
3. Barth, K., & Döring, N. (2022). Online sexual risks for children and adolescents: A systematic review. *Child Abuse & Neglect*, 126, 105–118. <https://doi.org/10.1016/j.chiabu.2022.105118>
4. Stoilova, M., Livingstone, S., & Nandagiri, R. (2019). Children's data and privacy online: Issues and challenges. London School of Economics and Political Science.
5. United Nations Committee on the Rights of the Child. (2021). General Comment No. 25 on children's rights in relation to the digital environment. UN Doc. CRC/C/GC/25.
6. Green, L., Holloway, D., & Livingstone, S. (2019). Regulating children's online risks: A comparative analysis. *New Media & Society*, 21(1), 20–39.
7. Montgomery, K. (2015). Youth and surveillance in the Facebook era: Policy interventions and social implications. *Television & New Media*, 16(2), 144–150.
8. Nyst, C. (2018). Children's rights and business in a digital world: Confronting corporate responsibility. *International Journal of Human Rights*, 22(3), 306–326.
9. Choudhury, N., & Singh, A. (2020). Cyber vulnerabilities and child safety: An Indian perspective. *Indian Journal of Law and Technology*, 16(1), 55–78.
10. Internet Watch Foundation. (2023). Annual report: Online child sexual abuse material. IWF.
11. Collier, B. (2021). Protecting children online: Balancing privacy, freedom, and safety. *Information & Communications Technology Law*, 30(3), 315–331.
12. Kidron, B., & Rudkin, A. (2021). Digital childhood: Addressing online harms. 5Rights Foundation.
13. United Nations Committee on the Rights of the Child. (2013). General Comment No. 16: State obligations regarding the impact of the business sector on children's rights. UN Doc. CRC/C/GC/16.
14. National Crime Records Bureau. (2023). Crime in India: Statistics on cybercrimes against children. Ministry of Home Affairs, Government of India.
15. Sharma, R., & Sinha, P. (2022). Examining child pornography laws in cyberspace: Indian and global perspectives. *Journal of Law and Technology Review*, 18(3), 67–89.
16. Council of Europe. (2001). Budapest Convention on Cybercrime. European Treaty Series No. 185.
17. Gasser, U., Maclay, C., & Palfrey, J. (2010). Working towards a deeper understanding of digital safety for children and young people in developing nations. Harvard Public Law Working Paper, No. 10-36.
18. UNESCO. (2021). Artificial intelligence and child rights: Opportunities and challenges. UNESCO.
19. Livingstone, S., & Stoilova, M. (2021). The 4Cs: Classifying online risk to children. *Communications Research*, 48(1), 1–20.
20. Berson, I. R., & Berson, M. J. (2019). Children's rights and digital citizenship. *International Journal of Child-Computer Interaction*, 22, 100–112.
21. Byrne, J., Kardefelt-Winther, D., Livingstone, S., & Stoilova, M. (2016). Global kids online research synthesis, 2015–2016. UNICEF Office of Research.
22. European Commission. (2022). EU strategy for a better internet for kids (BIK+). Publications Office of the European Union.
23. Wolak, J., Finkelhor, D., & Mitchell, K. (2018). Child sexual exploitation on the internet: Trends and emerging risks. Crimes Against Children Research Center.
24. OECD. (2021). Children in the digital environment: A global policy outlook. OECD Publishing.
25. United Nations. (1989). Convention on the Rights of the Child. United Nations Treaty Series, 1577, 3.
26. European Union. (2016). General Data Protection Regulation (GDPR). Regulation (EU) 2016/679.

27. Government of India. (2000). Information Technology Act, 2000 (No. 21 of 2000).
28. Government of India. (2012). Protection of Children from Sexual Offences Act, 2012 (No. 32 of 2012).
29. Government of India. (2023). Digital Personal Data Protection Act, 2023 (No. 22 of 2023).
30. Information Commissioner's Office. (2020). Age Appropriate Design Code: A code of practice for age-appropriate design. UK ICO.

Publisher's Note: The statements, opinions, findings, interpretations, and conclusions expressed in this article are solely those of the author(s) and do not necessarily reflect those of the Journal, its Editors, Editorial Board, reviewers, or Publisher. Responsibility for the accuracy and integrity of the scholarly content rests primarily with the author(s). The Journal, Editors, and Publisher exercise reasonable editorial and ethical oversight in accordance with the Journal's established policies; however, to the extent permitted by applicable law, they shall not be responsible for consequences arising from the use or interpretation of the information contained in the article. The Publisher remains neutral with regard to jurisdictional claims in published maps and institutional affiliations.

